The LWE-based key exchange – A Simple Provably Secure Key Exchange Scheme Based on the Learning with Errors Problem

Jintai Ding

University of Cincinnati

Key exchange protocol enables two users to exchange keys in untrusted channels without sharing secret materials in advance. The first and celebrated key exchange protocol is the Diffie-Hellman key exchange protocol [16] which is also a fundamental construction in public key cryptography. It is simple and elegant, and, after its invention, countless applications based on Diffie-Hellman key exchange protocol or the Diffie-Hellman problem were proposed.

Diffie and Hellman [16] also introduced the notion of public key encryption, and Rivest, Shamir and Adleman [27] gave the first concrete public key encryption scheme. Namely, the well-known RSA encryption. With public key encryption in hand, one can construct a key exchange protocol. Instantiating with the RSA algorithm, the construction produces a very efficient key exchange protocol. However, the encryption-type key exchange protocol may have an important side-effect in practice: This approach relies on the user's private key to protect all the session keys, anyone with access to a copy of the private key can also uncover the session keys and thus decrypt everything.

The Diffie-Hellman protocol offers an alternative algorithm to RSA for cryptographic key exchange. The Diffie-Hellman protocol generates more secure session keys that can't be recovered simply by knowing the user's private key, a protocol security feature called *forward security*. In order to decrypt all communication, now the adversary can no longer compromise just the user's private key, but the adversary has to compromise the session keys belonging to every individual communication session. In other words, using the Diffie-Hellman protocol, even an adversary knows the session key of some particular session, he still can not learn anything about the session keys established before this particular session. Actually, SSL also uses the Diffie-Hellman protocol to support forward security.

The motivation of this report is to build simple Diffie-Hellman like key exchange protocols based on lattices. Lattice-based public key cryptography has become a promising potential alternative to public key cryptography based on traditional number theory assumptions. One building block of lattice-based cryptography, especially in encryption, is the learning with errors (LWE) problem. After the introduction of LWE problem by Regev [26], it has attracted a lot of attentions in theory and applications due to its usage in cryptographic constructions with good provable secure properties. In a nutshell, the (decisional) LWE problem is to distinguish polynomially many noisy inner-product samples of the form $(\mathbf{a}, b \approx \langle \mathbf{a}, \mathbf{s} \rangle)$ from uniformly random ones, where $\mathbf{a} \leftarrow \mathbb{Z}_q^n$ and $\mathbf{s} \leftarrow \mathbb{Z}_q^n$ are uniformly random.[1] An attractive property of the LWE problem is that Regev [26] shows that to solve the average-case LWE problem is at least as hard as to (quantumly) solve some worst-case hard lattice problems. Many lattice-based primitives based on LWE have been discovered, such as public-key encryption [26,18,23], (hierarchical) identity-based encryption [18,1,15], functional encryption [3,2,9,19] and fully homomorphic encryption [12,11,10].

In the constructions mentioned above, a matrix form of the LWE problem is always used (i.e., need sufficient many samples). The drawback of that is it results in large (say quadratic) key size. To further improve the efficiency, Lyubashevsky, Peikert and Regev [24] introduced the ring learning with errors (RLWE) problem, which is to distinguish polynomially many noisy ring multiplications $(a, b \approx a \cdot s)$ from uniform distribution, where " $\cdot$" is the multiplicative operation over some ring.

[1] $\mathbf{s}$ is secret and remains the same in all the samples.

It's shown in [24] that to solve the RLWE problem is at least as hard as to solve some worst-case problems in *ideal* lattices, instead of general lattices.

What motivates the work in this report is to try to build a simple key exchange protocol using the basic idea of Diffie-Hellman protocol but based on the LWE and RLWE problem. There are already related works in [21,22,14,17], but as far as we know there is not yet until very recently any provably secure key exchange protocols based on the LWE problem as a direct generalization of the Diffie-Hellman key exchange protocol, which is elegant in terms of its simplicity. Our work was finished in 2012 [20]. Recent works on LWE-based Key exchange protocols [25], [8], [5], [7] are all variants of our protocol with minor modifications but some with significant contributions in concrete implementations.

To achieve our goal, we use the normal form of LWE problem suggested in [6] and introduce a new randomized method to eliminate bias, which may be of independent interest.

The key idea behind our new construction can be viewed as a way to share a secret given by the value of the bilinear function of two vectors $\mathbf{x}$ and $\mathbf{y}$ in $\mathbb{Z}_q^n$, where q, n are some integers, via the bilinear form:

$$Q(\mathbf{x}, \mathbf{y}) = \mathbf{x}^T \mathbf{A} \mathbf{y} = (\mathbf{x}^T \mathbf{A})\mathbf{y} = \mathbf{x}^T (\mathbf{A}\mathbf{y}),$$

where $\mathbf{A}$ is an $n \times n$ matrix in $\mathbb{Z}_q$. Surely in order to make the system provably secure, we need to introduce the small errors to achieve our goal. The main contribution of our work is to use this simple idea to build a simple and provably secure key exchange scheme. The idea of such an "noise" or "approximate" KE appeared long time ago like the work of Buchmann and Williams [13], and recently the work [4] using coding theory. A new fundamental contribution of ours, which is something very different from the DH KE is that we developed a new idea of "signal functions" as an additional tool needed to round the approximate value to a shared secret without affecting the security. Furthermore, we extend our construction further based on the RLWE problem. Our construction is a significant additional step in showing how versatile the LWE assumption can be.

Besides, we also give an interactive multiparty key exchange protocol. This protocol can be viewed as a generalization of our two party protocol. Although the provable security of the protocol seems plausible but we do not know how to do it, and we leave it as an open problem.

References

1. S. Agrawal, D. Boneh, and X. Boyen. Efficient lattice (h) ibe in the standard model. In *EUROCRYPT*, pages 553–572. Springer, 2010.
2. S. Agrawal, X. Boyen, V. Vaikuntanathan, P. Voulgaris, and H. Wee. Functional encryption for threshold functions (or fuzzy ibe) from lattices. In *PKC*, pages 280–297, 2012.
3. S. Agrawal, D. Freeman, and V. Vaikuntanathan. Functional encryption for inner product predicates from learning with errors. In *ASIACRYPT*, pages 21–40. Springer, 2011.
4. Carlos Aguilar, Philippe Gaborit, Patrick Lacharme, Julien Schrek, and Gilles Zemor. Noisy diffie-hellman protocols. PQC2010, Rum session, 2010. `https://pqc2010.cased.de/rr/03.pdf`.
5. Erdem Alkim, Lo Ducas, Thomas Pppelmann, and Peter Schwabe. Post-quantum key exchange - a new hope. Cryptology ePrint Archive, Report 2015/1092, 2015. `http://eprint.iacr.org/2015/1092`.
6. B. Applebaum, D. Cash, C. Peikert, and A. Sahai. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In *CRYPTO*, pages 595–618. Springer, 2009.
7. Joppe Bos, Craig Costello, Léo Ducas, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Ananth Raghunathan, and Douglas Stebila. Frodo: Take off the ring! practical, quantum-secure key exchange from lwe. Cryptology ePrint Archive, Report 2016/659, 2016. `http://eprint.iacr.org/2016/659`.
8. Joppe W. Bos, Craig Costello, Michael Naehrig, and Douglas Stebila. Post-quantum key exchange for the tls protocol from the ring learning with errors problem. Cryptology ePrint Archive, Report 2014/599, 2014. `http://eprint.iacr.org/2014/599`.
9. X. Boyen. Attribute-based functional encryption on lattices. In *TCC*, pages 122–142. Springer, 2013.
10. Z. Brakerski. Fully homomorphic encryption without modulus switching from classical gapsvp. In *CRYPTO*, pages 868–886. Springer, 2012.

11. Z. Brakerski, C. Gentry, and V. Vaikuntanathan. (leveled) fully homomorphic encryption without bootstrapping. In *ITCS*, pages 309–325, 2012.
12. Z. Brakerski and V. Vaikuntanathan. Efficient fully homomorphic encryption from (standard) lwe. In *FOCS*, pages 97–106. IEEE, 2011.
13. Johannes A. Buchmann and Hugh C. Williams. A key exchange system based on real quadratic fields. In *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*, pages 335–343, 1989.
14. R. Canetti, D. Dachman-Soled, V. Vaikuntanathan, and H. Wee. Efficient password authenticated key exchange via oblivious transfer. In *PKC*, pages 449–466. Springer, 2012.
15. D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert. Bonsai trees, or how to delegate a lattice basis. *EUROCRYPT*, pages 523–552, 2010.
16. W. Diffie and M. E. Hellman. New directions in cryptography. *Information Theory*, 22(6):644–654, 1976.
17. A. Fujioka, K. Suzuki, K. Xagawa, and K. Yoneyama. Strongly secure authenticated key exchange from factoring, codes, and lattices. In *PKC*, pages 467–484. Springer, 2012.
18. C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *STOC*, pages 197–206. ACM, 2008.
19. S. Gorbunov, V. Vaikuntanathan, and H. Wee. Attribute-based encryption for circuits. In *STOC*, pages 545–554. ACM, 2013.
20. Xiaodong Lin Jintai Ding, Xiang Xie. A simple provably secure key exchange scheme based on the learning with errors problem. Cryptology ePrint Archive, Report 2012/688, 2012. `http://eprint.iacr.org/2012/688`.
21. J. Katz and V. Vaikuntanathan. Smooth projective hashing and password-based authenticated key exchange from lattices. In *ASIACRYPT*, pages 636–652. Springer, 2009.
22. J. Katz and V. Vaikuntanathan. Round-optimal password-based authenticated key exchange. In *TCC*, pages 293–310. Springer, 2011.
23. R. Lindner and C. Peikert. Better key sizes (and attacks) for lwe-based encryption. In *CT-RSA*, pages 319–339, 2011.
24. V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. In *EUROCRYPT*, pages 1–23, 2010.
25. C. Peikert. Lattice cryptography for the internet. Cryptology ePrint Archive, Report 2014/070, 2014.
26. O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In *STOC*, pages 84–93. ACM, 2005.
27. R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.